FEDERAL AVIATION ADMINISTRATION

Aircraft Certification's Software and Digital Systems Safety (SDSS) Research Plan

July 1, 2005

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office as to its use.

Contents

1 INTRODUCTION......6

2 VERIFICATION AND VALIDATION TECHNIQUES......8

2.1 OBJECT-ORIENTED TECHNOLOGY (OOT) VERIFICATION (PART 3)......8
2.1.1 Project Description......8
2.1.2 Project Schedule/Deliverables......10
2.2 MC/DC ALTERNATIVES......10
2.2.1 Project Description......10
2.2.2 Project Schedule/Deliverables......11

3 COTS TECHNOLOGY IN COMPLEX & SAFETY-CRITICAL SYSTEMS.12

3.1 EFFECTS OF ACCELERATED SEMICONDUCTOR DEVICE WEAROUT......12
3.1.1 Project Description......13
3.1.2 Project Schedule/Deliverables......14
3.2 MICROPROCESSOR EVALUATIONS......16
3.2.1 Project Description......16
3.2.2 Project Schedule/Deliverables......18
3.3 ENVIRONMENTAL QUALIFICATION OF INDUSTRIAL / COMMERCIAL ELECTRONIC COMPONENTS......18
3.3.1 Project Description......18
3.3.2 Project Schedule/Deliverables......18
3.4 BURN-IN TESTING CRITERIA OF CRITICAL ELECTRONIC EQUIPMENT......18
3.4.1 Project Description......19
3.4.2 Project Schedule/Deliverables......19
3.5 OBSOLESCENCE AND LIFE CYCLE MAINTENCE OF AVIATION ELECTRONICS......19
3.5.1 Project Description......19
3.5.2 Project Schedule/Deliverables......19

4 INTEGRATION AND DEVELOPMENT TECHNIQUES FOR HIGHLY-INTEGRATED AIRCRAFT SYSTEMS......20

4.1 COMPONENT INTEGRATION......20
4.1.1 Project Description......20
4.1.2 Project Schedule/Deliverables......21
4.2 MODEL-BASED DEVELOPMENT ASSESSMENT CRITERIA......21
4.2.1 Project Description......21
4.2.2 Project Schedule/Deliverables......22
4.3 REQUIREMENTS ENGINEERING MANAGEMENT......22
4.3.1 Project Description......23
4.3.2 Project Schedule/Deliverables......24
4.4 AIRCRAFT SYSTEM LEVEL IMPACTS ON SOFTWARE DEVELOPMENT ASSURANCE LEVEL DETERMINATION......25
4.4.1 Project Schedule/Deliverables......25
4.4.2 Project Schedule/Deliverables......25

4.5 SOFTWARE TOOL QUALIFICATION CRITERIA........25
4.5.1 Project Description........25
4.5.2 Project Schedule/Deliverables........26

5 ONBOARD NETWORK SECURITY AND INTEGRITY........26

5.1 LOCAL AREA NETWORKS (LANS) IN AIRCRAFT........26
5.1.1 Project Description........26
5.1.2 Project Schedule/Deliverables........29
5.2 DATABUS EVALUATION CRITERIA........30
5.2.1 Project Description........31
5.2.2 Project Schedule/Deliverables........32
5.3 TRANSFER OF AVIATION DATA ON THE INTERNET........33
5.3.1 Project Description........33
5.3.2 Project Schedule/Deliverables........33

6 COMPLEX ELECTRONIC HARDWARE TECHNIQUES AND TOOLS.....33

6.1 COMPLEX HARDWARE DEVICE ASSURANCE........33
6.1.1 Project Description........33
6.1.2 Project Schedule/Deliverables........34
6.2 QUALIFICATION OF COMPLEX ELECTRONIC HARDWARE TOOLS........34
6.2.1 Project Description........34
6.2.2 Project Schedule/Deliverables........34
6.3 VERIFICATION COVERAGE ANALYSIS OF COMPLEX ELECTRONIC HARDWARE.....35
6.3.1 Project Description........35
6.3.2 Project Schedule/Deliverables........35

7 RELIABILITY MODELING........35

7.1 SOFTWARE SERVICE HISTORY (RELIABILITY MODELS)........35
7.1.1 Project Description........36
7.1.2 Project Schedule/Deliverables........36
7.2 SAFETY ENGINEERING APPROACHES FOR SOFTWARE........36
7.2.1 Project Description........36
7.2.2 Project Schedule/Deliverables........37

APPENDIX A – HISTORY OF SDSS RESEARCH........38

Tables

Table 1. List of SDSS TCRG Members...........................**Error! Bookmark not defined.**
Table 2. Effects of Accelerated Semiconductor Device Wearout Deliverables 15
Table 3. Microprocessor Evaluations Deliverables 18
Table 4. Component Integration Deliverables 21
Table 5. Requirement Engineering Management Deliverables 24
Table 6. Local Area Network Deliverables...29
Table 7 Databus Evaluation Criteria Deliverables...32

Acronyms

AACE	Airworthiness Assurance Center of Excellence
AAR	Office of Aviation Research Service
AAR-400	Airport and Aircraft Safety Research and Development Division
AAR-470	Flight Safety Branch
ACE-111	Regulations & Policy Branch, Small Airplane Directorate
ACE-117C	Systems and Flight Test Branch, Chicago ACO, Small Airplane Directorate
AFS	Aviation Flight Standards Service
AFS-302	TBD, Continuous Airworthiness Maintenance Division, Flight Standards Service
AIR	Aircraft Certification Service
AIR-100	Aircraft Engineering Division
AIR-106N	CSTA for Aircraft Computer Software
AIR-120	Technical Standards Branch
AIR-130	Avionics Systems Branch
ANE-110	Engine & Propeller Standards Staff, Propulsion Directorate
ANM-100	Transport Airplane Directorate
ANM-103N	CTSA for Advanced Avionics Electrical
ANM-111	Airplane & Flight Crew Interface Branch, Transport Airplane Directorate
ANM-113N	CSTA for Advanced Control Systems
ANM-114N	CSTA for Aeronautical Communications
ARP	Aerospace Recommended Practice
ASICs	Application Specific Integrated Circuits
ASU	Arizona State University
ASW-110	Rotorcraft Standards Staff, Rotorcraft Directorate
ASW-170	Rotorcraft Certification Office, Rotorcraft Directorate
AVSI	Aerospace Vehicle Systems Institute
CFR	Code of Federal Regulations
COTS	Commercial Off-The-Shelf
CPDLC	Controller-Pilot Data Link Communication
CSTA	Chief Scientific and Technical Advisor
EP	Envelope Protection
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FBL	Fly-By-Light
FBW	Fly-By-Wire
FC	Flight Critical
FG&C	Flight Guidance and Control
FMS	Flight Management System
FPA	Flight Path Angle
FPGAs	Field Programmable Gate Arrays
FY	Fiscal Year

GA	General Aviation
GPS	Global Positioning System
IMA	Integrated Modular Avionics
HUD	Head-Up Display
HUMS	Health Usage and Monitoring Systems
LaRC	Langley Research Center
MAC	Media Access Controller
MMI	Man Machine Interface
NAS	National Air Space
NASA	National Aeronautics and Space Administration
NIC	Network Interface Card
OS	Operating System
OOT	Object Oriented Technology
OOTiA	OOT in Aviation
PFD	Primary Flight Display
PIO	Pilot-induced Oscillation
PLDs	Programmable Logic Devices
RPD	Research Project Description
RTCA, Inc.	formerly Radio Technical Commission for Aeronautics
RTOS	Real-Time Operating System
SAE	Society for Automotive Engineers
SC	Special Committee
SDSS	Software and Digital Systems Safety
SRAM	Static Random Access Memory
SSH	Software Service History
TAC	Thrust Asymmetry Compensation
TCRG	Technical Community Representative Group
TECS	Total Energy Control System
THCS	Total Heading Control System
UAV	Unmanned Air Vehicle
VNAV	Vertical Navigation
WAAS	Wide Area Augmentation System
WG	Working Group

1 Introduction

The purpose of this plan is to summarize the planned research activities of the Federal Aviation Administration (FAA) Aircraft Certification Service (AIR) to address the software and flight critical digital systems certification and approval needs. The goal of the Software and Digital Systems Safety (SDSS) Project is to maintain or improve aircraft safety by conducting research in the area of advanced digital (software-based and programmable logic-based) airborne systems technology. The goal of this project is met by publishing technical data, reports, compliance and verification methods, and certification techniques that, when used to develop policy and guidance materials, will assist both the FAA and industry in meeting their safety objectives.

The field of digital systems is constantly changing and is becoming more complex and pervasive within aircraft systems. To address the safety of aircraft, AIR must keep abreast of the changing technology. This project will assist and educate FAA, both AIR and the Flight Standards Service (AFS), and industry specialists in understanding this technology and assessing how it may be safely employed in flight essential and flight critical systems such as fly-by-wire (FBW) flight controls, navigation and communication equipment, autopilots, and other avionics functions. Failure of these highly complex systems could lead to aircraft incidents or accidents.

The risk of not performing the identified research will hamper the ability of both FAA and industry to evaluate emerging, highly complex digital hardware and software for use in advanced flight controls and avionics systems. Consequently, certification specialists will find it difficult to properly assess proposed subsequent aircraft and avionics designs which employ this technology in flight essential and flight critical applications. Further, they will not be able to determine if certification policy or criteria need to be revised to accommodate this new technology. **If the policy or criteria do need revision without that revision occurring, a reduction in the level of safety could result with the possibility of accidents and/or incidents.**

An additional risk of not performing this research is a reduction in the ability to develop, validate, and improve certification methods. This would inhibit improvements in the timeliness and cost reduction of certifying aircraft employing advanced digital airborne systems.

This plan is developed with the input of Chief Scientific and Technical Advisors (CSTAs); Technical Specialists; policy staff; RTCA, Inc., Society for Automotive Engineers (SAE), and European Organization for Civil Aviation Equipment (EUROCAE) special committees (SCs); and international certification authorities. The members of the SDSS Technical Community Representative Group (TCRG) are listed below.

Table removed for privacy purposes, since this plan will be posted on the SDSS Project (RPD #560) website sponsored by the Flight Safety Branch, AJP-6350.

The plan addresses three areas of focus: software, digital hardware, and digital systems. The plan is divided into seven major requirement areas, each having a number of tasks:

1. Safe and Cost-Effective Verification and Validation Techniques (see section 2)
2. COTS Technology in Complex and Safety-Critical Systems (see section 3)
3. Integration and Development Techniques for Highly-Integrated Aircraft Systems (see section 4)
4. Onboard Network Security and Integrity (see section 5)
5. Complex Electronic Hardware Development Techniques (see section 6)
6. Reliability Modeling (see section 7)

This plan is a “living” document and will be updated annually, at minimum, or sooner should important requirements emerge.

2 Verification and Validation Techniques

Verification and validation at the software, hardware, and system levels is required to ensure that systems comply with the regulations and perform their intended functions. As technology advances and becomes more complex, the verification and validation process changes. This research will consider effective verification and validation techniques including verification and validation of software, hardware, and system requirements.

2.1 Object-Oriented Technology (OOT) Verification (Part 3)

In FY 2000, an Object Oriented Technology (OOT) verification task was initiated with National Aeronautics and Space Administration (NASA) Langley Research Center (LaRC) as the primary researcher. Parts 1 and 2 (FY 2000 and FY 2001) of the task resulted in a report summarizing issues resulting from the effect of certain features of OOT on structural coverage. The report from this effort is available on the FAA's web-site http://www.faa.gov/certification/aircraft/av-info/software/software.htm.

In Parts 1 and 2, project focus was on documenting issues and acceptance criteria to address structural coverage of OOT. This effort was used as input into the FAA's "Handbook for Object-Oriented Technology in Aviation" which was published in October 2004. This Handbook is also available on the FAA's website http://www.faa.gov/certification/aircraft/av-info/software/software.htm. The purpose of Part 3 is to further address areas where the use of OOT impacts structural coverage with particular emphasis on: (1) confirmation (verification) of data coupling and control coupling and (2) sufficiency of structural coverage. In addition, other verification issues outside structural coverage will be identified.

2.1.1 Project Description

The purpose of this project is to provide input to the FAA for developing policy and guidance for the use of object-oriented technology (OOT) in aviation (OOTiA) systems and to support harmonization with international certification authorities on the use of OOTiA. Developers of airborne software are beginning to widely use OOT. Previous FAA research and two OOTiA workshops with industry indicate that there are some areas of OOT verification that are still a concern in safety-critical systems. Two particular areas are: (1) data and control coupling and (2) structural coverage at the object code level. Each concern is briefly described below:

Data and control coupling: Data coupling and control coupling are not unique to OOT. However, data coupling and control coupling relationships can be far more complicated and obscure in OOT than they are in traditional (functionally-developed) systems/ software. One impact on data coupling and control coupling is in the nature of OOT. OOT encourages the development of many small, simple methods to perform the services provided by a class. Most of the control flow is moved out of the source code through the use of polymorphism and dynamic binding. In essence, the control flow, and thereby the control coupling, will become implicit in the source code, as opposed to being explicit. There is a similar effect on the data flow, and thereby the data coupling. OOT also encourages hiding the details of the data representation (i.e., attributes) behind an abstract class interface. Suggested "best practice" is that attributes of an object should be private, and access to them only provided through the methods appropriate to the class of the object Being able to access attributes only through methods makes the interaction between two or more objects implicit in the code.

Structural coverage at the object code level: Several applicants using OOT are proposing to meet Objective #5 of DO-178B/ED-12B Table A-7 (MC/DC) by performing coverage of the object code instead of the traditional source code coverage approach. Because of the modeling approach used in OOT, some people also contend that coverage should be performed at the object code level for all software levels (i.e., levels A, B, and C) in OOT. The following issues need to be better understood:

- Adequacy of coverage at the object code level to ensure that it is at least as good as the current coverage at the source code level for non-OO software;
- Sufficiency of structural coverage at the source code level for OOT to determine if it is at least as good as current coverage at the source code level for non-OO software
- Need for coverage at the object code level for all software levels to determine application of structural coverage to OOT projects.

The contractor will perform the following tasks for each of the three phases:

Phase 1.

1. Conduct a literature search to identify reference material on:
    a. The use of OOT in commercial aviation and the current and proposed verification practices for that OOT.
    b. Current and proposed interpretations and practices for the confirmation of software data coupling and control coupling and how those interpretations and practices relate to OOT.
    c. Current and proposed interpretations and practices for the structural coverage of OOT software and how coverage at the object code level satisfies the objectives of RTCA DO-178B with the clarifications given in RTCA DO-248B and CAST position papers.
2. Develop a research plan for the project. This plan will be reviewed and updated based on the information learned in developing each deliverable.
3. Conduct a survey through the Boeing DERs to determine from Boeing's airborne software supplier base the state-of-the-industry concerning:
    a. The use of OOT in commercial aviation and the current and proposed verification practices for that OOT.
    b. Current and proposed interpretations and practices for the confirmation of software data coupling and control coupling and how those interpretations and practices relate to OOT.

c. Current and proposed interpretations and practices for the structural coverage of OOT software and how coverage at the object code level satisfies the objectives of RTCA DO-178B with the clarifications given in RTCA DO-248B and CAST position papers.

Phase 2.

Identify the language specific and/or tool specific issues and acceptance criteria concerning the confirmation of data coupling and control coupling in OOT.

Phase 3.

1. Identify the language specific and/or tool specific issues and acceptance criteria concerning the structural coverage of OOT software at the source code and object code levels.
2. Identify the concerns and open issues concerning OOT software verification that identify issues requiring further research.

2.1.2 Project Schedule/Deliverables

The work will be divided into three phases beginning in FY 2003 and have a total duration of not longer than 36 months.

TABLE 1. OOT VERIFICATION (PART 3) DELIVERABLES

#	Description of Product	Delivery Date/ Months after Contract Award
1	Status Report	Bi-Monthly
2	Literature Search/Summary	2 months
3	Research Plan	3 months
4	Briefing on Plan	3.5 months
5	Phase 1 Report/Handbook	12 months
6	Phase 2 Report/Handbook	24 months
7	Phase 3 Report/Handbook	36 months

2.2 MC/DC Alternatives

The purpose of this project is to evaluate alternates to modified condition/decision coverage (MC/DC) and other DO-178B structural coverage objectives. The output of this research will be used as input to DO-178C and/or future FAA policy and guidance.

2.2.1 Project Description

DO-178B requires structural coverage for software Levels A, B, and C (see objectives 5 through 7 of Table A-7). Unlike most of the DO-178B objectives, which state “what” should be done, objectives 5 through 7 of Table A-7 prescribe “how” it should be done. In particular, objective 5 of Table A-7 states “Test coverage of software structure (modified condition/decision) is achieved.” Modified condition/decision coverage (MC/DC) is really a “how” objective; i.e., it provides a specific technique for carrying out the structural coverage. Recent research efforts have revealed that other approaches may address the concern of identifying unreached code to the same level of efficacy as MC/DC (e.g., coupled-cause MC/DC (CCM) and Operator Coverage Criterion (OCC).

The purpose of this task is to consider acceptable alternatives to MC/DC that obtain the same overall intent. CCM and OCC should be considered, as well as other appropriate techniques. Additionally, the task should develop criteria for evaluating other techniques in the future to determine if it meets the same intent as MC/DC. I.e., generalized evaluation criteria should be evaluated, so that research is not needed for every possible method. This effort builds upon the verification tools task and past structural coverage analysis research.

This task will strive to answer the following questions, as a minimum:

- What is the overall intent of MC/DC?
- What methods achieve the same intent?
- Do CCM and OCC satisfy objective 5 of Table A-7?
- What is criteria for determining if a technique satisfies objective 5 of Table A-7?
- What might be a better statement of objective 5 of Table A-7? I.e., how might it be stated to be more “what” focused, rather than “how”?

2.2.2 Project Schedule/Deliverables

The performance period for this task was originally expected to start in FY 2007 and last for 24 months. However, since the outcome of this project is needed to support DO-178B revision, funding beginning in FY 2006 for 12 or 18 months total will be considered. The deliverable will be a report documenting acceptable alternatives to MC/DC and generalized criteria for evaluating techniques to determine equivalency to MC/DC.

3 COTS Technology in Complex & Safety-Critical Systems

Manufacturers desire to use commercial-off-the-shelf (COTS) software and hardware to reduce development costs and potentially improve quality. Since there is often no insight into the original COTS component development and verification, approaches are needed in order to safely implement COTS into safety-critical aviation products. This research considers a number of COTS-related concerns that are currently facing the aviation industry and the regulators. Resulting information will be used to update existing policy and guidance.

3.1 Effects of Accelerated Semiconductor Device Wearout

The purpose of this project is to develop methods to evaluate the mechanisms and accommodate the effects of accelerated semiconductor device wearout on avionics system design, production, and support; and to account for shorter device lifetimes in avionics system safety and reliability analysis.

The solid-state electronics industry is characterized by relentless pressures to expand and improve functions; reduce costs; and reduce design and development time. As a result, device feature sizes have shrunk to the nanometer range, and design life cycles to less than five years. These trends are increasing, rather than abating.

Until recently, semiconductor device lifetimes could be measured in decades, which was essentially infinite with respect to their required service lives. It was therefore not critical to quantify the device lifetimes exactly, or even to understand them completely. For avionics applications, it was reasonable to assume that all devices would have constant, and relatively low, failure rates throughout the life of the system, and this assumption is built into avionics design, as well as reliability and safety analysis processes.

Recently, it has become apparent that semiconductor device and process technology have progressed to the point that the device manufacturers can design and produce products that will wear out in less than a decade. Lifetime goals of 3-5 years are now practical for high-volume end-use products, such as laptop computers and cellular telephones. These types of applications dominate the semiconductor device market, and device manufacturers are designing their products with these goals in mind. (Preliminary calculations for metal migration failures indicate that devices designed with current design rules may have lifetimes of less than ten years. Other potential failure mechanisms include time dependent dielectric breakdown and hot carriers.)

Unfortunately, the semiconductor device industry devotes its scarce technical resources to design and production for high-volume applications. The level of effort devoted to reliability assessment is sufficient to assure that their products will be reliable in the major end-use applications, and little else. This impacts the aerospace industry in a significant way, because the supply chain for aerospace semiconductor devices has essentially disappeared, and aerospace customers must rely on components designed and produced for high-volume end-use applications.

Avionics systems must operate for long service lifetimes in rugged environments. The industry is highly regulated and the consequences of failure are high. Life-limited electronic components, with poorly-understood failure mechanisms, could be the source of serious problems in system reliability, availability, supportability, cost, and possibly even safety.

Lack of knowledge regarding semiconductor device failure mechanisms and shorter device lifetimes are of grave concern to the aerospace industry. It is vital for us to understand the impacts of smaller device features and newer materials. We also must understand the impacts of the resulting non-constant failure rates on system safety and reliability assessment calculation methods, and on the results of those calculations.

3.1.1 Project Description

The purpose of this project is to evaluate current and future technology, develop guidelines, and evaluate reliability and safety assessment methods.

3.1.1.1 Evaluate Current and Future Technology

Evaluate the present and future state of the art of commercial semiconductor device designs and production processes. Understand and quantify the potential failure modes and mechanisms that would result if the devices were operated in aerospace environments for the required service lives. Conduct a critical review of the literature to determine models used for the key failure mechanisms (time-dependent-dielectric breakdown, electromigration, hot carriers, etc.). Perform experimental work to verify the models and determine constants for aerospace applications, using samples of devices with gate oxide and feature sizes that represent current and future device technology (obtained through contacts at NIST and NASA). Develop models that are capable of extrapolation to the specific operating conditions experienced in air and space environments.

3.1.1.2 Develop Guidelines

Based on the results of the above work, develop aerospace system design guidelines that take into account the shorter device lifetimes, and the failure modes and mechanisms of the devices. If necessary, develop tools to evaluate the above effects; and develop guidelines for customized semiconductor device selection and qualification for aerospace applications.

3.1.1.3 Evaluate Reliability and Safety Assessment Methods

Review current aerospace system reliability and safety assessment methods, and evaluate their capability to accommodate the failure patterns expected of future semiconductor devices. Review methods currently in use in other industries with critical safety requirements, e.g., nuclear, and determine their applicability to aerospace systems with state of the art semiconductor devices. If necessary, modify avionics system reliability and safety assessment methods to account for limited semiconductor device lifetimes, and for the resulting non-constant failure rates.

3.1.2 Project Schedule/Deliverables

The FAA is funding this research through the Aviation Vehicle Systems Institute (AVSI), a non-profit consortium of members including the government agencies FAA and DoD and the industry members of Boeing, Goodrich, Honeywell, Rockwell Collins, and Smiths Aerospace. The contractor/researcher for this effort is the University of Maryland (UMD). It is currently scheduled to be a three-year task; however, it may be expanded to a four-year task. The task started in 2002 and will continue to the end of 2005, at which time a decision will be made to end or continue the task into the fourth year. Actual tasks and associated deliverables for the first three years are shown below:

Year 1:

1. Conduct literature search and consult with device manufacturers to determine likely failure mechanisms of future semiconductor devices in avionics applications.
2. Develop models to estimate expected lifetimes of future avionics.
3. Verify mechanisms and models by use of existing avionics systems data, experimental results, or consultation with device manufacturers.
4. Estimate cost impact of early device wear out.

Year 2:

1. Develop guidelines and test methods to design and develop aerospace systems to accommodate effects of early device wear out.
2. Perform accelerated life testing on SRAM parts to fit the wear out model.
3. Modify and enhance the derating model to accommodate actual data and compare to field failures to further validate the models.

Year 3:

This project will leverage off the results of Phases 1-3. The project objectives are:

1. Develop a handbook outlining key semiconductor device attributes that can impact avionics system design, and recommend methods to manage them. Chapters include (1) Foreword; (2) Introduction; (3) CMOS Failure Mechanisms and Reliability Models; (4) Electronic Packaging Reliability; (5) Competing Models of Electronic Systems with Multiple Failure Mechanisms; (6) Failure Rate-Based SPICE Reliability

Simulation; (7) Accelerated Life Tests. Appendices include (A) Competing Models; (B) Component Reliability Data (C) SRAM Acceleration Test Case Study. This will be the responsibility of the University of Maryland.

2. Using the handbook, develop a practical design guide for use by avionics system designers during product development. The guide will be used for leading edge semiconductor devices, and will address tradeoffs among speed, temperature, voltage, and operating life to ensure reliable performance of the system throughout its life. This will be the responsibility of the participating member organizations.
3. Work with semiconductor device to further understand the meaning of short service life, and to understand the impact of future device technology on avionics system design, production, and support. This will be the responsibility of the participating member organizations.
4. Conduct accelerated reliability testing of selected semiconductor devices: (A) Complete SRAM testing at JPL; ((B) Motorola (0.15 and 0.090µ – 100 pcs. per technology); (C) Intel (0.13 and 0.090µ- 30 pcs. per technology); (D) Tower (0.35 and 0.18µ – 100 pcs. per technology).

Deliverable 1. Handbook (UMC Contractor)
1.1. Second quarter, 2005: Chapters 1, 2, 3, 4, 5, and appendices A, B, C
1.2. Third quarter, 2005: Chapters 6, 7
1.3. Fourth quarter, 2005: Final draft

Deliverable 2. Guidelines (AVSI TEAM)
2.1. Second quarter, 2005: Outline and preliminary draft (Done by PMC Working Group)
2.2. Fourth quarter, 2005: Final draft. (Done by PMC Working Group)

Deliverable 3. Semiconductor Manufacturer Information (AVSI TEAM)
3.1. Fourth quarter, 2005: Final report. (Done by PMC Working Group)

Deliverable 4. Test Results (UMC Contractor)
4.1. First quarter, 2005: JPL report.
4.2. Second quarter, 2005: Final test plan for Motorola, Intel, and Tower.
4.3. Fourth quarter, 2005: Complete tests and issue final report.

TABLE 1. EFFECTS OF ACCELERATED SEMICONDUCTOR DEVICE WEAROUT DELIVERABLES

Phase 3: Objectives (months from program start)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1. Handbook						1.1			1.2			1.3
2. Guidelines						2.1						2.2
3. Manufacturer Data												3.1

4. Test results			4.1			4.2						4.3

3.2 Microprocessor Evaluations

To date, relatively little criteria has been documented on how to evaluate microprocessors for safety assurance. The aviation community tends to use well-proven microprocessors. However, objective criteria for determining what is a high-risk vs. low-risk microprocessor does not exist. Both DO-178B and DO-254 fail to document how microprocessors should be assured. The purpose of this project is to investigate microprocessor use in the industry, to document assessment criteria for microprocessors, and to document safety concerns for microprocessors.

3.2.1 Project Description

Dense electronic packaging has been developed for portable consumer devices such as cellular phones and pagers, as well as in memory cards and other applications with consumer, automotive and industrial uses. The large volume of sales for microprocessors and advanced device packaging in these products have made their way into the aviation domain. These microprocessor devices have the general concept of reducing the size, weight and power of a product and adding capability by using advanced design and component packaging techniques. However, the design and packaging techniques have led to the use of concepts, such as caching and pipelining, which can affect system performance with regards to determinism and safety. For example, use of caching can affect timing analysis and task scheduling.

In fiscal year 2003, a small task was carried out in conjunction with the COTS real-time operating system (RTOS) project. The report entitled “Commercial Off-The-Shelf (COTS) Real Time Operating Systems (RTOS) and Architectural Considerations” summarizes the effort and is available on the FAA’s web-site http://www.faa.gov/certification/aircraft/av-info/software/software.htm.
The study focused on the PowerPC, since it is a processor used in many airborne projects. The study identified many features of the microprocessor and associated RTOS services that could pose some potential safety concerns for the system under development. The study revealed that the use of cache memory, especially with pipelining, increases the complexity and accuracy of the worst-case execution time (WCET) analysis, which may affect the measure of a system’s determinism.

The Certification Authorities Software Team (CAST) completed a paper entitled “Addressing Cache in Airborne Systems and Equipment” (number CAST–20) which is available on the FAA’s web-site http://www.faa.gov/certification/aircraft/av-info/software/software.htm. This paper considered some of the concerns of using caching in airborne systems. Some of the concerns are summarized below:

- Many airborne systems contain multiple software functions of different software levels – cache memory is a common resource used by all the software functions executing on that microprocessor. Therefore, providing protection mechanisms and partitioning between those functions can be very challenging and necessitates thorough analyses and complete robustness testing of the approach and implementation of cache memory management.

- Many cache management approaches rely heavily on commercial-off-the-shelf (COTS) hardware components, such as memory management units (MMUs) and watchdog timers, that, if relatively new and untested, may not have a history of reliable and predictable performance integrity.
- In many safety-critical real-time systems, certain “critical” code functions must execute at a specific frequency (or when certain events occur) reliably, while other software functions in the same application may have less time-critical need for control of the processor and its resources. Obviously, safety-related time-critical code must execute reliably and timely, independent of other function’s (sharing the processor resources) needs.
- Other concerns revolve around WCET analysis complexity and accuracy when using cache memory.

Most microprocessors are accepted on aircraft through a combination of service history and testing. Per DO-178B, requirements-based tests are performed on the target computer (which includes the processor) to give assurance that the software works properly in the actual environment. This activity demonstrates the microprocessor functionality. However, as more complex microprocessors are used, more complex hardware is integrated, and fully partitioned systems are implemented, the concern of a defined process for microprocessor acceptance is needed. DO-254 could apply to microprocessors but it may prove to be cost prohibitive. This research will focus on some of the current microprocessors being proposed on aircraft and establish evaluation critieria.. The effort will briefly consider the applicability of RTCA/ DO-254 to microprocessors. The emphasis of the effort will be to document potential safety concerns when using modern processors on aircraft, and to propose potential approaches for addressing those safety concerns. The effort will build upon the use of microprocessors in past aircraft certification efforts (e.g., the Boeing 777) but will also consider issues of modern processors (e.g., the PowerPC) and their usage integrated modular avionics. The project will provide practical techniques for use by aircraft manufacturers, avionics developers, certification authorities, and other stakeholders. Another goal of the project is to provide criteria for the level of rigor required for various levels of systems that use microprocessors (i.e., to provide an approach for scaling the criteria depending on the functional criticality of the processor). This task was started in FY 2004 as part of the Aerospace Vehicle Systems Institute (AVSI) with participating industry members Boeing, Smiths Aerospace, and BAE Systems.

Specific project tasks are to:

- Review current utilization of microprocessors and computational processing components, in general, in the aviation industry.
- Assess the suitability of DO-254 to microprocessors.
- Document the potential safety issues that occur when using modern microprocessors (e.g., the PowerPC and Intel processors). This will build upon existing findings.

- Document approaches for evaluating microprocessors to ensure that the safety issues have been addressed. This might include criteria for service experience and component testing that may be used to evaluate microprocessors.
- Document evaluation criteria specific to microprocessors that may be used to comply with DO-254 or serve as input to an FAA Advisory Circular or an update to DO-254.

3.2.2 Project Schedule/Deliverables

This project was started in FY 2004 and will continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

This project will build upon the FAA report ("Commercial Off-The-Shelf (COTS) Real Time Operating Systems (RTOS) and Architectural Considerations"), the CAST paper ("Addressing Cache in Airborne Systems and Equipment"), and RTCA/DO-254 ("Design Assurance Guidance For Airborne Electronic Hardware").

TABLE 2. MICROPROCESSOR EVALUATIONS DELIVERABLES

#	**Description of Product**	**Delivery Date/ Months after Contract Award**
1	Project Plan (allow 1 month for FAA input)	2
2	Status Reports	quarterly
3	First Year Report	31 July 2005
4	Final Report	31 July 2006

3.3 Environmental Qualification of Industrial / Commercial Electronic Components

Component manufacturers are not designing electronic devices to meet aerospace environmental conditions. The FAA needs methods to analyze and test these devices to determine if they will function reliably in more severe environmental conditions than those specified by the manufacturer.

3.3.1 Project Description

3.3.2 Project Schedule/Deliverables

This project is expected to start in FY 2008 and continue for three years. The deliverable will be one or more reports to be used as input for policy and guidance development.

3.4 Burn-In Testing Criteria of Critical Electronic Equipment

FAA does not currently require the use of burn-in tests to eliminate electronic equipment with high infant mortality or manufacturing defects from entering service. The FAA needs test methods, typically temperature and vibration tests to identify and eliminate defective equipment if it is used in critical applications such as fly by wire engine and flight control systems.

3.4.1 Project Description

3.4.2 Project Schedule/Deliverables

This project is expected to start in FY 2008 and continue for three years. The deliverable will be one or more reports to be used as input for policy and guidance development.

3.5 Obsolescence and Life Cycle Maintence of Aviation Electronics

In the past, general aviation aircraft have been able to rely on the availability of stable parts, e.g., electrical/electronic/pneumatic/mechanical/etc or TSOd indicators/ instruments, even for decades. This stability/availability has helped make the lower end of the aviation spectrum fairly affordable. Now, with the increasing use of digital electronic instruments/ indicators, that may not be the case. This change could impact the life cycle maintenance (i.e., continued airworthiness) and incumbent ownership costs for an entire new generation of GA aircraft, and to an extent, transport aircraft as well.

3.5.1 Project Description

This task would look into how the rapidly changing, fast-paced, commercially driven (i.e., by consumer electronics such as digital computers/cameras/video/ sound/phones/ PDAs/etc) hardware development community will impact the life cycle of aviation electronics (avionics), especially for lower end General Aviation (GA) applications, by quickly obsolescing spares/availability of such things as processors/ASICs/PLDs/ memory/interfaces/etc.

Such a task might also look into considerations for changing the model of implementing corrective actions (i.e., Airworthiness Directives) since the possibility of more frequent "recalls" due to denser hardware/software/functionality will challenge the status quo of often having the aircraft owner pay for the repair work, even when due to design/build errors!

3.5.2 Project Schedule/Deliverables

This project is expected to start in FY 2009 and continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

4 Integration and Development Techniques for Highly-Integrated Aircraft Systems

4.1 Component Integration

The purpose of this project is to provide input to the FAA for developing policy and guidance on component integration and to support harmonization with international certification authorities in implementing component integration. Integrated Modular Avionics (IMA) systems use both software and hardware components to implement aircraft functionality. Components may be software, hardware, or a combination of software and hardware. Components may be commercially purchased or developed in-house. The FAA is working with RTCA Special Committee #200 (SC-200) and EUROCAE working group #60 (WG-60) to define guidelines for development and certification of IMA systems. The SC-200/WG-60 effort, previous FAA research, and actual certification projects indicate that integration of components into the IMA system is a safety and certification concern. The real-time operating system (RTOS) is a specific component that is of concern for integration into the IMA systems. This research effort will consider three aspects of integration:

1. Integration of the RTOS into an IMA system.
2. Integration of components into IMA systems.
3. Verification of component integration into IMA systems.

4.1.1 Project Description

Pratt & Whitney, as the contractor, will perform the following tasks for each of the three phases:

Phase 1:

- Develop a plan for this research effort to include all three phases.
- Perform a literature survey and document reference resources for the overall research effort to include all three phases.
- Identify issues and acceptance criteria for integration of RTOS into IMA systems.
- Document this Phase 1 information in the form of a report to the FAA and a handbook that can be made available to industry.

Phase 2:

- Identify issues and acceptance criteria for integration of components into IMA systems.
- Document this Phase 2 information in the form of a report to the FAA and a handbook that can be made available to industry.

Phase 3:

- Identify issues and acceptance criteria for verification of component integration into IMA systems.
- Identify concerns and future research needs related to integration, components, and IMA systems.
- Document the Phase 3 information in the form of a report to the FAA and a handbook that can be made available to industry.

4.1.2 Project Schedule/Deliverables

This three phase project started in FY 2003 for a duration of not longer than 36 months.

TABLE 3. COMPONENT INTEGRATION DELIVERABLES

#	Description of Product	Delivery Date/ Months after Contract Award
1	Status Report	Bi-Monthly
2	Literature Search/Summary	2 months
3	Research Plan	3 months
4	Briefing on Plan	3.5 months
5	Phase 1 Report/Handbook	12 months
6	Phase 2 Report/Handbook	24 months
7	Phase 3 Report/Handbook	36 months

4.2 Model-Based Development Assessment Criteria

4.2.1 Project Description

Historically, specifications for aircraft subsystems have been mainly based on English language (informal) text. Many manufacturers are attempting to use a new approach for aircraft specification – one that is more graphical/model-based. The goal is to improve requirements validation and implementation. Many of the models are integrated with code generators. The tool generates code from the model without human intervention. The approach for validating and applying DO-178B to model-based development is unclear. (This approach is also closely related to OO.) There are a number of questions or issues that arise:

- Are models adequate to be called “requirements” by themselves (i.e., do they describe “what” is being built)? Or, are text-based requirements needed to supplement the models, since the models represent implementation details?
- What constitute systems and high-level software requirements in a model-based development?
- If low-level software requirements are not generated, what additional activities are needed to meet the intent of DO-178B?

- If the model is at the systems requirements level, what extra activities do systems personnel need to perform in order to ensure that the requirements are accurate, etc.? I.e., What modifications to the system life cycle are required to ensure that overall system integrity is not compromised (since the system and software life cycles are being merged)?
- At what level of requirements must verification be performed?
- If tool qualification is required, what objectives must be applied to the tool?
- If commercial tools are used, how can qualification be carried out?

The purpose of this project is to explore the approaches to model-based development being considered by industry, document the technical and certification issues, and document potential approaches for addressing the technical and certification issues.

4.2.2 Project Schedule/Deliverables

The performance period for this task was originally expected to start in FY 2007 and last for 24 months. However, since the outcome of this project is needed to support DO-178B revision, funding beginning in FY 2006 for 12 or 18 months total will be considered. The deliverable will be a report documenting the issues identified and potential approaches for addressing them.

4.3 Requirements Engineering Management

The advent of new technology, particularly in the area of Integrated Modular Avionics (IMA) suites, has allowed "reusable" designs in which some components of both hardware or software of an IMA system will be used on multiple aircraft applications, some of which may be under initial development and/or major updates and modifications simultaneously. That is, some IMA hardware and software components installed on one aircraft type and configuration will be used on different aircraft types and configurations which use similar, but not identical, software loads, programmed electronic hardware devices, and IMA system configurations. The management of requirements becomes even more challenging when multiple developers and teams are involved.

RTCA DO-178B (invoked by AC 20-115B as an acceptable means of compliance for the software aspects of certification, and hereafter referred to as DO-178B) and Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754 contain some guidance for system requirements capture and validation. However, neither document specifically addresses guidance for managing system requirements for highly complex and integrated systems, such as an IMA-type of architecture.

The complexity of the IMA architecture makes it crucial that system, hardware, and software requirements are properly managed, controlled, verified, and validated by the applicant throughout the development and operational use of the IMA system.

The purpose of this research task is to determine methods that enable successful management, control, integration, verification, and validation of system and software requirements that may be developed by multiple entities. The ability to establish requirements traceability from the system-level requirements to the software requirements, particularly from high-level to low-level requirements, and to track requirements refinement and changes are of particular concern.

4.3.1 Project Description

The goal of this task is to determine methods that enable successful management, control, integration, verification, and validation of system and software requirements that may be developed by multiple entities. The output of this task will be used as input for development of FAA policy, regulations (if deemed needed), and guidance materials. This research project will also enhance material in ARP 4754, ARP 4761 and the output of RTCA's IMA committee (Special Committee #200, which is jointly acting with EUROCAE working group #60). Additionally, the following sub-objectives will be pursued:

- What are the current practices of manufacturers in the areas of requirements management?
- What are safety and certification concerns of requirements management, particularly as integration increases?
- What are the best practices regarding requirements management, control, integration, verification, and validation of system and software requirements?
- What are the best practices regarding requirements traceability when multiple entities are involved?
- What approaches can be implemented to address certification concerns?

Rockwell Collins, as the contractor, will perform the following tasks for each of the two phases:

<u>Phase 1: Identify current practices, determine safety and certification concerns, and draft best practices</u>. Identify the current practices of manufacturers in the areas of requirements management; determine the safety and certification concerns of requirements management, particularly as integration increases; document preliminary best practices in the areas of requirements management, control, integration, verification, validation, including traceability when multiple entities are involved and validation at company/ organizational boundaries; and provide a report summarizing the research process and results.

<u>Phase 2: Validate, update, and complete best practices; and complete report/handbook</u>. Update research plan and survey (as needed, based on Phase 1 progress); validate, update, and complete best practices regarding requirements management, control, integration, verification, and validation of software and system requirements; determine the best practices regarding requirements traceability when multiple entities are involved;

determine best practices regarding requirements validation at company/organizational boundaries encountered in the development of a software product; determine approaches that can be implemented to address certification and safety concerns; provide final report (includes 1-year and 2-year research process and results); and provide a handbook of best practices.

4.3.2 Project Schedule/Deliverables

This project started in FY 2004 and will continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

TABLE 4. REQUIREMENT ENGINEERING MANAGEMENT DELIVERABLES

Phase 1: Deliverables/ Objectives (months from task start)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1. Develop plan		X										
2. Status report		X		X		X		X		X		
3. Perform literature search and industry survey			X									
4. Kick-off briefing			X									
5. Identify current practices					X							
6. Determine safety and certification concerns							X					
7. Draft best practices for requirements engineering										X		
8. End of Phase 1 briefing										X		
9. Document in a report												X
Phase 2: Deliverables/ Objectives (mos from phase 2 start)												
10. Status report		X		X		X		X		X		
11. Update plan and literature search (as needed)		X										
12. Beginning of Phase 2 briefing		X										
13. Validate, update and complete requirements engineering best practices								X				
14. Determine certification and safety approaches									X			
15. End of task briefing									X			
16. Complete final report (inc. year-1 & year-2 results)												X
17. Complete best practices												X

handbook												

4.4 Aircraft System Level Impacts on Software Development Assurance Level Determination

4.4.1 Project Schedule/Deliverables

This project will investigate the determination or mitigation of appropriate software and hardware development assurance levels via consideration of the overall aircraft level system design/architecture. That is, it will consider how aircraft level system hardware/software design attributes (e.g., architecture, redundancy, independence, partitioning, dissimilarity, etc.) affect the determination of the appropriate software assurance levels at the LRU or function levels while considering the FHA/SSA processes' conclusions (this topic is related to DO-178B sections 2.2 and 2.3).

4.4.2 Project Schedule/Deliverables

This project is expected to start in FY 2008 and continue for two years. The deliverable will be one or more reports to be used as input for FAA and industry consideration.

4.5 Software Tool Qualification Criteria

4.5.1 Project Description

The FAA has conducted research in the area of software tools (e.g., verification and development tool research). Additionally, the FAA has been overseeing a number of tool projects and conducted a Software Tools Forum. The two tool research tasks and the Software Tool Forum report indicate a need for continued research in the area of software tools.

Additionally, RTCA/SC-205 has been charged with modifying DO-178B or creating supplemental guidance. There will be considerable emphasis on the modification of DO-178B’s tool qualification criteria. This research effort will provide technical input to the committee updating DO-178B in order to ensure that the criteria implemented in future guidance is technically sound.

This research effort will consider recommendations from the final verification tools research report, the final development tools research report, and the Software Tools Forum report. The focus will be on the tools of higher priority (as identified in the Software Tools Forum report). The software tools forum identified the following five priorities:

1. Development Tool Qualification Criteria Needs to Be Modified
2. Criteria for Model-Based Development Needs to Be Established
3. Qualification Criteria that Enables Qualification to be Carried from One Program to Another Needs to be Developed

4. Different Approaches to Autocode Generator Usage and Qualification Need to be Developed and Documented
5. Integration Tools Pose New Challenges that Need to Be Addressed

This research effort will explore these five areas to propose potential solutions.

4.5.2 Project Schedule/Deliverables

The performance period for this task was originally expected to start in FY 2007 and last for 24 months. However, since the outcome of this project is needed to support DO-178B revision, funding beginning in FY 2006 for 12 or 18 months total will be considered. The deliverable will be a report documenting the issues identified and potential approaches for addressing them.

5 Onboard Network Security and Integrity

5.1 Local Area Networks (LANs) in Aircraft

5.1.1 Project Description

This task will investigate safety and security aspects of local area networks (LANs) onboard the aircraft. With the introduction of the network to the aircraft, concerns arise of how security breaches may affect safety. This project will consider network security concerns and propose recommendations for addressing those concerns in the safety and certification environment. Two major areas will be investigated: (1) the potential security risks of an onboard network that could impact safety and (2) the means for mitigating the security risks in the certification environment (i.e., a network security assurance process).

Traditionally, the airborne software has remained secure, because of the limited access and closed system approach. To date, updates to airborne software have typically been performed in one of two ways: (1) in a laboratory by an approved alteration/repair station, or (2) on the aircraft through a proprietary port with approved personnel. However, the current technology is changing. The advances in computing ability, network reliability, and wireless technology have led aircraft manufacturers and operators to pursue onboard networks to operate, update, and maintain the aircraft. The use of such networks onboard aircraft raises concerns as to how security breaches to these networks could impact aircraft safety. This task will consider network security concerns and propose recommendations for addressing those concerns in the safety and certification environment. The results of the effort will be considered as input to future FAA policy, guidance, and regulations.

A paper completed by the Certification Authorities Software Team (CAST) documented nine concerns regarding the onboard networks being proposed and the future trends that seem to be emerging in aviation. The nine CAST concerns are documented below:

- Concern 1 - Connection of Multiple Domains: Current large transport aircraft are considering connecting several domains via a network. The concern is that aircraft manufacturers are considering connecting the avionics, airline, and cabin networks into a single aircraft integrated network. This could have a number of safety impacts, such as hackers posing as passengers trying to access the flight software or even hackers on the ground attempting to access the flight software, if a public IP is used.
- Concern 2 - Integrated Modular Avionics (IMA) Implementation: IMA systems introduce a number of potential security risks that are not common in the traditional federated system. IMA systems are designed to be flexible, reconfigurable, and field loadable. Airborne software will likely be modified in the field, onboard the aircraft, using a network facility. The concern is that airborne software could be improperly accessed or even corrupted through the network or or through the field loading process. RTCA Special Committee #200 and EUROCAE Working Group #60 are developing guidance to begin addressing this concern.
- Concern 3 - Using Public IPs: Aircraft manufacturers desire to make broadband Internet Protocol (IP) available to the aircraft. At least some manufacturers are planning to use a public IP. The concern is that if the aircraft uses a public IP, it will become a target for hackers all over the world. If the airborne software is connected to this network, safety could be impacted.
- Concern 4 - Electronic Flight Bags: Electronic flight bags (EFBs) come in many shapes and forms. Currently, most EFBs are laptop computers that are used by the pilots for advisories and information. The concern is that the advances in EFB technology and capability will eventually result in the EFBs connecting to the aircraft. The concern is that viruses or corrupt software could be downloaded onto EFBs off-board the aircraft. When the EFBs are connected to the aircraft, they could negatively impact the airborne software.
- Concern 5 - Updating Security Protection Software: Another concern is the process for updating security protection software. Maintaining a secure network requires frequent updates, in order to address new viruses and threats. However, updating an aircraft network would require a modification to a type-certificated product. Therefore, the update must go through the certification process. In many cases, the change may be considered minor; however, the update may take time. Updating the aircraft software frequently could become a large time and cost burden for manufacturers, operators, and regulators.
- Concern 6 - Responding to Security Breaches: Another concern is how responses to security breaches would occur. Some contend that the aircraft would be able to address a breach on its own. However, other believe that ground support may be needed to respond to a security problem, since security experts may not be onboard every flight. Currently, airlines or regulators have not set up such infrastructure.
- Concern 7 - Access to Aircraft Data: Additional potential security threats could be initiated from employees of airlines, aircraft manufacturers, and their suppliers. Many security solutions involve denial of access to sensitive data or physical

locations to unauthorized persons; these solutions are not purely based on technological issues and must also be considered.

- Concern 8 - Adequacy of Existing Regulations: Additionally, the terms "safety" and "security" are not synonymous. Although Title 14 of the Code of Federal Regulations (CFR) part 25.1309 could be interpreted to include security threats as a "foreseeable condition", this was not the original intent of the rule. If the FAA is to address security threats, a new rule may be required. Existing rules and policy for type certification of aircraft do not address security concerns. Some of the techniques of the safety assessment process, particularly the Functional Hazard Assessment, could be used as a staring point to evaluate potential security threats, but the requirements for security protection should probably be separate from safety requirements. The means providing protection from security threats may be different than the means used to provide failure protection.
- Concern 9 - Ground to Air Communication: There are a number of ground to air communications with the onboard networks that are also of concern (e.g., connection to the Internet, datalink, etc).

The Boeing Company, as the contractor, will perform the following tasks for each of the two phases:

Phase 1 Description:

The goal of the first phase is to document potential security threats associated with onboard networks that could affect safety. The following questions should be considered while carrying out this phase:

- What are safety concerns of onboard networks?
- What are security concerns of onboard networks?
- If the safety and security concerns identified conflict with one another, how can both safety and security be addressed without compromising the other?
- What are some solutions to those safety and security issues?
- How can the security aspects be addressed in the certification environment?
- How can certification concerns be addressed?

For this effort, the contractor will perform the following tasks: Identify current industry trends in implementing onboard networks, identify safety and security issues associated with onboard networks, document initial acceptance criteria, and provide a 1 report summarizing the research process and results.

Phase 2 Description:

The goal of the second phase is to validate and complete the acceptance criteria started in phase 1 and to document a network security assurance process. The network security assurance process will include a framework that can be used by certification authorities and industry to ensure that networks onboard the aircraft will not negatively impact the safety of the aircraft. The security assurance process should supplement existing safety assessment approaches (e.g., SAE ARP 4754 and ARP 4761). The output of this task will be considered by the FAA as input for development of FAA policy, regulations, and guidance materials for industry regarding the use of LANs in aircraft. The following questions should be considered while carrying out this phase:

- Are current regulations adequate to address security concern?
- How does the security assurance process fits into the overall certification process, including ties to the safety assessment (XX.1309, ARP4754, ARP4761, DO-178B, and DO-254)?
- What should a Network Security Assurance process contain to enable onboard networks to meet XX.1309?
- How will continued airworthiness be addressed for onboard networks and how will regular maintenance be performed in the certification environment?
- How can it be ensured that systems connected to the onboard network cannot negatively impact safety?
- What should the process be for updating security protection software?
- How can security breaches be handled?

For this effort, the contractor will perform the following tasks: Update research plan and survey, validate and update the first year's acceptance criteria, develop the safety assurance process (which should implement the criteria), provide final report (includes phase 1 and 2 research process and results), and provide a practical handbook summarizing the acceptance criteria and safety assurance process to address certification and safety concerns.

5.1.2 Project Schedule/Deliverables

This project started in FY 2004 and will continue for two years. The first phase will last 12 months and will focus on the potential security risks of onboard networks that affect safety. The second phase will last 12 months and will develop criteria for assessing and addressing the risks (i.e., a network security assurance framework).

TABLE 5. LOCAL AREA NETWORK DELIVERABLES

Phase 1: Deliverables/ Objectives (months from phase 1 effort start)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1. Develop plan		X										
2. Status report		X		X		X		X		X		
3. Perform literature search/ industry survey			X									
4. Kick-off briefing			X									
5. Identify security and safety										X		

issues, and initial acceptance criteria												
6. End of Phase 1 briefing										X		
7. Document in a report												X
Phase 2: Deliverables/ Objectives (months from phase 2 effort start)												
8. Status report		X		X		X		X		X		
9. Update plan and literature search (as needed)		X										
10. Beginning of Phase 2 briefing		X										
11. Validate, update and, complete acceptance criteria					X							
12. Document an overall network security assurance acceptance process (using the acceptance criteria in #11 above).								X				
13. End of task briefing									X			
14. Complete final report and develop handbook												X

5.2 Databus Evaluation Criteria

Manufacturers are proposing a number of databuses for first-time use in aircraft. The need for increased bandwidth and decreased wiring weight drive this trend. A databus provides numerous physical/logical configurations of avionics architecture, data units/packets, message traffic, etc. This allows considerable design flexibility for system/sub-system engineers. Without extensive configuration management control across many manufacturers, vendors, and integrators, this flexibility can make the establishment of a type design, eventual determinations of compliance, and maintaining continued airworthiness extremely difficult. The most widely used aviation databuses (i.e., ARINC 429 and 629) are not considered adequate for expanding future aviation applications. Therefore, several databuses are being considered for use in aircraft. The FAA and industry have performed research in the area of Ethernet, which is being proposed for large transport aircraft. However, for general aviation aircraft (business jets and smaller aircraft), a number of different communication technologies are being considered (such as, CAN (controller area network), ByteFlight, TTP/C (time-triggered protocol), SAFEbus, FlexRay, FireWire, and others). There is a need for generalized criteria that applies to multiple technologies being proposed as aircraft databuses.

The purpose of this task is to document evaluation criteria for databuses to be used in aviation products. The criteria will be considered in future FAA policy and guidance.

5.2.1 Project Description

The goal of this task is to develop objective criteria for evaluating databus technology in safety-critical applications. Certification authorities and industry will use the criteria to ensure that onboard databuses perform their intended functions and do not negatively impact aircraft safety. The output of this research will be used by the FAA as input to policy, guidance, and regulations, as deemed necessary.

In this project, a number of potential databuses will be evaluated in order to develop assessment criteria that can be applied to aircraft projects using new databuses. Certification Authorities Software Team (CAST) Position Paper CAST-16 "Databus Evaluation Criteria" (available at:http://www2.faa.gov/certification/aircraft/av-info/software/software.htm) documents a number of general criteria for evaluating databuses. This task should build upon the CAST paper and provide a list of issues and proposed solutions each of the following areas, as they apply to databus technology:

- Safety and reliability,
- Data integrity,
- Performance,
- Design and development assurance,
- Electromagnetic compatibility and other environmental issues,
- Validation/verification/testing,
- Configuration management,
- Continued airworthiness and maintenance,
- Certification and/or qualification procedures,
- Security, and
- Other items related to databus safety.

For this task, Honeywell International will perform the following tasks for each of the two phases:

Phase 1: Perform literature and industry survey, document databus certification and safety issues, and propose draft evaluation criteria to address the issues . Assess the usage and plans regarding databus technology by surveying literature and the industry. Based on the literature and industry input, identify the primary certification concerns related to new databus technology, with focus on safety. Document preliminary evaluation criteria to address the major concerns. Develop a plan for validating and completing the criteria in the second phase.

Phase 2: Validate and complete the evaluation criteria in a report and handbook. Update the research plan for Phase 2 (based on lessons learned in Phase 1) and search/ survey (as needed). Validate, update, and complete the evaluation criteria started in Phase 1 by applying the criteria to one or more aviation databuses. Provide a final report (including year-1 and year-2 data) and a databus evaluation handbook.

5.2.2 Project Schedule/Deliverables

This project started in FY 2004 and will continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

TABLE 6 DATABUS EVALUATION CRITERIA DELIVERABLES

Phase 1: Deliverables/ Objectives (months from phase 2 task start)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1. Develop plan		X										
2. Status report		X		X		X		X		X		
3. Perform literature search			X									
4. Kick-off briefing			X									
5. Perform literature search and industry survey					X							
6. Document primary certification, performance, and safety issues of databus technology							X					
7. Draft evaluation criteria to address the issues in item 6 and develop plan to complete criteria in Phase 2.									X			
8. End of Phase 1 briefing										X		
9. Document research results and draft evaluation criteria in a Year-1 report.												X
Phase 2: Deliverables/ Objectives (months from phase 2 task start)												
10. Status report		X		X		X		X		X		
11. Update plan and literature search, base on Phase 1 lessons learned.		X										
12. Beginning of Phase 2 briefing		X										
13. Identify databus(es) to be evaluated.				X								
14. Validate the evaluation criteria by applying it to one or more aviation databuses						X						

15. Update the evaluation criteria						X						
16. End of task briefing									X			
17. Complete final report (including year-1 and year-2 information)												X
18. Complete a databus evaluation handbook												X

5.3 Transfer of Aviation Data on the Internet

5.3.1 Project Description

Because of convenience and timeliness, some aviation manufacturers desire to begin transferring their airborne software over the internet or by e-mail. The purpose of this research effort is to identify the potential safety and certification issues of such a process and to propose solutions.

Some of the questions to be answered are:

- What are safety and security concerns of transferring flight data over the internet or by e-mail?
- What are some solutions to those safety issues?
- How can certification concerns be addressed?

5.3.2 Project Schedule/Deliverables

- This project should start in FY 2007 and continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

6 Complex Electronic Hardware Techniques and Tools

6.1 Complex Hardware Device Assurance

The main impact of DO-254 is intended to be on the design of complex hardware items. However, AC 20-152 addresses only a subset of complex devices, e.g., PLDs, FPGAs, ASICs, custom micro-coded components, and similar electronic hardware. Since this AC does not specifically address all complex hardware items per DO-254, the FAA needs methods to evaluate these other complex devices for safety assurance.

6.1.1 Project Description

DO-254 provides guidance applicable to a variety of hardware items including: line replaceable units; circuit board assemblies; custom-micro-coded components, such as ASICs, PLDs, and associated macro functions; integrated technology components such as hybrids and multi-chip modules; and COTS components. However, AC 20-152 addresses only a subset of these devices, specifically, PLDs, FPGAs, ASICs, custom micro-coded components, and similar electronic hardware. This project will explore the types of hardware items beyond those identified in AC 20-152 that are used by industry and approaches to evaluating them for safety assurance with respect to intended function and compliance with airworthiness requirements.

6.1.2 Project Schedule/Deliverables

This project is expected to start in FY 2007 and continue for three years. The deliverable will be one or more reports to be used as input for policy and guidance development.

6.2 Qualification of Complex Electronic Hardware Tools

RTCA DO-254 provides guidance for the development and approval of complex electronic hardware (e.g., programmable logic devices (PLDs), application specific integrated circuits (ASICs), etc.). DO-254 provides some guidance on qualification of tools; however, there are issues regarding tool qualification that remain unanswered. This project will seek to identify and address tool qualification issues for complex electronic hardware development and verification tools. The output of this project will be used to develop policy and guidance.

6.2.1 Project Description

This research will study the approaches that should be taken for both development (e.g. affecting the target system) and verification (e.g. affecting the analysis of the target system verification) tools for certification levels A, B, C and D. It will be based on guidelines proposed in DO-254.

Questions considered as a starting point for this project include:
1) What are approaches that should be taken to qualify verification and development tools?
2) What techniques are currently used to 'qualify' tools to other approval bodies?
3) Can Tool Service History be used and, if so, how?
4) Can a Testing Maturity Model play a role in tool qualification?

The tasks to be carried out are:
1) Research how tools are qualified in other safety domains.
2) Assess the Testing Maturity Model effects on tool qualification
3) Study tool service history as a practice basis

6.2.2 Project Schedule/Deliverables

This project is expected to start in FY 2006 and continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

6.3 Verification Coverage Analysis of Complex Electronic Hardware

RTCA DO-254 provides guidance for the development and approval of complex electronic hardware. It defines the verification process that assures that the hardware item implementation meets the requirements and discusses that verification coverage analysis should be performed. However, sufficiency of coverage analysis is not succinctly defined and the use of COTS complicates the situation. The output of this project will be used to develop policy and guidance.

6.3.1 Project Description

This research will study the level of testing needed to ensure that embedded logic on a chip is sufficiently exercised. It will consider advanced verification methods such as elemental analysis.

Questions considered as a starting point for this project include:
1) How can it be shown that the embedded logic on the chip has been fully exercised even when advanced methods are used?
2) What is “sufficiency of testing” and how can it be demonstrated for levels A, B, and C?
3) How may verification coverage be demonstrated if advanced methods are not used?
4) What provides a level of confidence similar to DO-178B structural coverage analysis?

6.3.2 Project Schedule/Deliverables

This project is expected to start in FY 2008 and continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

7 Reliability Modeling

7.1 Software Service History (Reliability Models)

In 2000-2001, the FAA sponsored a research project in software service history (SSH) that resulted in a handbook and report. This project also identified two areas of SSH where additional research is needed:

a. Elimination of inconsistencies in DO-178B between the use of service history and the prohibition of software reliability use in the assessment of system safety;
b. Development and publication of guidelines for using specific software reliability models only if the models can be justified by means of tool qualification.

7.1.1 Project Description

This project will take an objective look at software reliability and its relationship to software reliability models and software service history. An important difference exists between software reliability demonstrated by software service history, as opposed to software reliability predicted by software reliability models. Service history is an actual demonstration of some degree of reliability, whereas reliability modeling yields a prediction based on certain estimation input parametrics (e.g., development methodology used, organizational maturity, complexity of application domain, lines of code, etc.). The values obtained via reliability modelling can be considered best guess scientific projections and should not inspire the same confidence as service history values unless it can be shown otherwise. An instance that might demonstrate model reliability would be when an application was developed according to a model's parametric estimations and then demonstrated an actual service history commensurate with that estimate.

In addition, software based component reliability models have many customizable component derating schemes that have not been generally reviewed and accepted within the FAA. Some applicants are using these automated reliability tools, such as relex, to derive the FTA primary event failure probabilities since the tools are available and MIL-STD-217 is not being maintained.

Criteria for acceptable reliability models will be identified.

7.1.2 Project Schedule/Deliverables

This project should start in FY 2008 and last two years. The project will result in a report and handbook that will be used as the input for policy and guidance on the use of reliability models and software service history.

7.2 Safety Engineering Approaches for Software

The purpose of this study will be to scientifically determine if parts of the RTCA/DO-178B could be reduced or eliminated by using safety engineering practices.

7.2.1 Project Description

The field of safety and reliability engineering has existed for many years and has a long record of applicability to hardware. However, a number of aviation manufacturers desire to expand these methods (e.g., fault trees, failure mode and effects analysis, etc.) to use in software applications. Currently, FAA Advisory Circular AC 20-115B recognizes RTCA/DO-178B as a means, but not the only means, of compliance to Code of Federal Regulations (CFR), Title 14 (14 CFR) XX.1301 and XX.1309 (where XX might be 23, 25, 27, 29, or 33). Software approval using safety engineering practices has been limited, because of the limited understanding of this field (i.e., there is little scientific documentation of how effective these methods are when applied to software).

Some of the questions to be answered are:

1. Can some RTCA/DO-178B objectives be reduced or eliminated by use of safety engineering approaches?
2. If so, what objectives, for what software levels, and how would the “credit” be documented?
3. What safety engineering techniques offer the most benefit for software?
4. What are the certification issues of applying safety engineering techniques to software engineering?
5. What are some potential steps to be taken to address those certification risks?

7.2.2 Project Schedule/Deliverables

This project should start in FY 2008 and continue for two years. The deliverable will be one or more reports to be used as input for policy and guidance development.

Appendix A – History of SDSS Research

Published reports from SDSS research are available, where possible, on the FAA software website at http://av-info.faa.gov/software. To date, the following reports are available on the website:

- DOT/FAA/CT-91/1 - Software Quality Metrics
- DOT/FAA/AR-95/31 - Design, Test, and Certification Issues for Complex Integrated Circuits
- DOT/FAA/AR-01/41 - Review of Pending Guidance and Industry Findings on Commercial Off-The-Shelf (COTS) Electronics in Airborne Systems
- DOT/FAA/AR-01/18 - An Investigation of Three Forms of the Modified Condition Decision Coverage (MCDC) Criterion
- DOT/FAA/AR-01/26 - Commercial Off-The-Shelf (COTS) Avionics Software Study
- DOT/FAA/AR-01/125 - Software Service History Report
- DOT/FAA/AR-01/116 - Software Service History Handbook
- NASA/TM-2001-210876 - A Practical Tutorial on Modified Condition/Decision Coverage
- DOT/FAA/AR-02/113 - Issues Concerning the Structural Coverage of Object-Oriented Software
- DOT/FAA/AR-02/118 - Study of Commercial Off-The-Self (COTS) Real-Time Operating Systems (RTOS) in Aviation Applications
- DOT/FAA/AR-03/51 – Simulation and Flight Test Assessment of Safety Benefits and Certification Aspects of Advanced Flight Control Systems
- DOT/FAA/AR-03/77 – Commercial Off-The-Shelf Real-Time Operating System and Architectural Considerations